Interference Search 09/707,433

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	35	"FIRST DIGITAL SIGNATURE".CLM. AND "SECOND DIGITAL SIGNATURE".CLM. AND "PUBLIC KEY".CLM. AND AUTHENTICAT$3.CLM.	US-PGPUB; USPAT	OR	OFF	2006/01/10 16:38
L2	19	1 AND CERTIFICATE.CLM.	US-PGPUB; USPAT	OR	OFF	2006/01/10 16:38
L3	4	2 AND PIN.CLM.	US-PGPUB; USPAT	OR	OFF	2006/01/10 16:39

updated search 09/707,433

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	35	"FIRST DIGITAL SIGNATURE".CLM. AND "SECOND DIGITAL SIGNATURE".CLM. AND "PUBLIC KEY".CLM. AND AUTHENTICAT$3.CLM.	US-PGPUB; USPAT	OR	OFF	2006/01/10 16:49
L2	19	1 AND CERTIFICATE.CLM.	US-PGPUB; USPAT	OR	OFF	2006/01/10 16:38
L3	4	2 AND PIN.CLM.	US-PGPUB; USPAT	OR	OFF	2006/01/10 16:40
L4	954	"DIGITAL SIGNATURE" AND "PUBLIC KEY CERTIFICATE" AND AUTHENTICAT$3 AND (PIN OR ID)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/01/10 16:41
L5	254	4 AND DIGEST	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/01/10 16:41
L6	208	5 AND SIGNATURES	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/01/10 16:42
L7	12	6 AND "SECOND DIGITAL SIGNATURE"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/01/10 16:45

updated search 09/706,433

PORTAL USPTO

Subscribe (Full Service) Register (Limited Service, Free) Login

Search: The ACM Digital Library The Guide

"digital signature" and "public key certificate" and authenticat$ SEARCH

THE ACM DIGITAL LIBRARY

Feedback Report a problem Satisfaction survey

Terms used **digital signature** and **public key certificate** and **authenticat$3** and **pin**

Found **191** of **169,166**

Sort results by relevance

Display results expanded form

Save results to a Binder

Search Tips

Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 191 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Relevance scale

1 On-line e-wallet system with decentralized credential keepers

Stig Frode Mjølsnes, Chunming Rong

February 2003 **Mobile Networks and Applications**, Volume 8 Issue 1

Publisher: Kluwer Academic Publishers

Full text available: pdf(240.23 KB) Additional Information: full citation, abstract, references, index terms

We propose a generalization of the architecture of an electronic wallet, as first developed in the seminal European research project CAFE. With this model you can leave most of the content of your electronic wallet at the security of your residential electronic keeper, while roaming with your favorite mobile terminals. Emerging mobile handsets with both short range Bluetooth and cellular GPRS communications provide a sufficient communication platform for this electronic wallet architecture. Howe ...

Keywords: digital credentials, e-wallet architecture, mobile commerce, payment protocols, privacy

2 Authentication in distributed systems: theory and practice

Butler Lampson, Martín Abadi, Michael Burrows, Edward Wobber

November 1992 **ACM Transactions on Computer Systems (TOCS)**, Volume 10 Issue 4

Publisher: ACM Press

Full text available: pdf(3.37 MB) Additional Information: full citation, abstract, references, citings, index terms, review

We describe a theory of authentication and a system that implements it. Our theory is based on the notion of principal and a "speaks for" relation between principals. A simple principal either has a name or is a communication channel; a compound principal can express an adopted role or delegated authority. The theory shows how to reason about a principal's authority by deducing the other principals that it can speak for; authenticating a channel is one important application. We ...

Keywords: certification authority, delegation, group, interprocess communication, key distribution, loading programs, path name, principal, role, secure channel, speaks for, trusted computing base

3 Authentication in distributed systems: theory and practice

Butler Lampson, Martín Abadi, Michael Burrows, Edward Wobber
September 1991 **ACM SIGOPS Operating Systems Review , Proceedings of the thirteenth ACM symposium on Operating systems principles SOSP '91**, Volume 25 Issue 5
Publisher: ACM Press

Full text available: pdf(2.33 MB) Additional Information: full citation, abstract, references, citings, index terms

We describe a theory of authentication and a system that implements it. Our theory is based on the notion of principal and a "speaks for" relation between principals. A simple principal either has a name or is a communication channel; a compound principal can express an adopted role or delegation of authority. The theory explains how to reason about a principal's authority by deducing the other principals that it can speak for; authenticating a channel is one important application. We use the th ...

4 Digital certificates: a survey of revocation methods

Petra Wohlmacher
November 2000 **Proceedings of the 2000 ACM workshops on Multimedia**
Publisher: ACM Press

Full text available: pdf(455.31 KB) Additional Information: full citation, abstract, references, citings, index terms

Digital certificates form a basis that allows entities to trust each other. Due to different constraints, a certificate is only valid within a specific period of time. Coming from several threats, there are important reasons why its validity must be terminated sooner than assigned and thus, the certificate needs to be revoked. This paper provides a classification of revocation methods and gives an overview of the main methods like CRL, CRS, CRT, and OCSP. If and in which way a revocation meth ...

Keywords: CRL, CRS, CRT, OCSP, X.509, attribute certificate, digital certificate, public-key certificate, revocation

5 Payments and banking with mobile personal devices

Amir Herzberg
May 2003 **Communications of the ACM**, Volume 46 Issue 5
Publisher: ACM Press

Full text available: pdf(152.82 KB) html(31.60 KB) Additional Information: full citation, abstract, references, citings, index terms, review

Mobile devices enable secure, convenient authorization of e-banking, retail payment, brokerage, and other types of transactions.

6 Security issues in ATM networks

Danai Patiyoot, S. J. Shepard
October 1999 **ACM SIGOPS Operating Systems Review**, Volume 33 Issue 4
Publisher: ACM Press

Full text available: pdf(1.08 MB) Additional Information: full citation, abstract, index terms

This paper presents a survey of existing solutions aiming to secure communications over ATM network. Details are given about: the security services offered, their placement within ATM protocol reference model, the mechanism to negotiate security services, techniques to provides synchronisation and key exchange protocol. Additionally, this paper proposes a new ATM security solution.

Keywords: ATM, security

7 Strong password-only authenticated key exchange

David P. Jablon

October 1996 **ACM SIGCOMM Computer Communication Review**, Volume 26 Issue 5

Publisher: ACM Press

Full text available: pdf(1.52 MB) Additional Information: full citation, abstract, citings, index terms

A new simple password exponential key exchange method (SPEKE) is described. It belongs to an exclusive class of methods which provide authentication and key establishment over an insecure channel using only a small password, without risk of offline dictionary attack. SPEKE and the closely-related Diffie-Hellman Encrypted Key Exchange (DH-EKE) are examined in light of both known and new attacks, along with sufficient preventive constraints. Although SPEKE and DH-EKE are similar, the constraints a ...

8 Untraceability in mobile networks

Didier Samfat, Refik Molva, N. Asokan

December 1995 **Proceedings of the 1st annual international conference on Mobile computing and networking**

Publisher: ACM Press

Full text available: pdf(1.20 MB) Additional Information: full citation, references, citings, index terms

Keywords: CDPD, GSM, alias, anonymity, authentication, location privacy, mobility, security

9 Papers: On the validity of digital signatures

Jianying Zhou, Robert Deng

April 2000 **ACM SIGCOMM Computer Communication Review**, Volume 30 Issue 2

Publisher: ACM Press

Full text available: pdf(586.65 KB) Additional Information: full citation, abstract, references

An important feature of digital signatures is to serve as non-repudiation evidence. To be eligible as non-repudiation evidence, a digital signature on an electronic document should remain valid until its expiry date which is specified by some non-repudiation policy. As signature keys may be compromised and the validity of signatures may become questionable, additional security mechanisms need to be imposed on digital signatures. This paper examines the mechanisms for maintaining the validity of ...

Keywords: digital signature, non-repudiation, secure electronic commerce

10 Digital signatures: can they be accepted as legal signatures in EDI?

Patrick W. Brown

December 1993 **Proceedings of the 1st ACM conference on Computer and communications security**

Publisher: ACM Press

Full text available: pdf(809.34 KB) Additional Information: full citation, abstract, references, citings, index terms

Digital Signature (DS) technology may be employed to produce legally enforceable signatures in Electronic Data Interchange (EDI) among computer users within the same general guidelines and requirements as those developed for handwritten signatures on paper. Digital signature technology promises assurance at least equal to written signatures. From a legal standpoint, this assurance remains to be tested in the

evidentiary process. Business policies for organizational use of this technology ar ...

Keywords: EDI, cryptography, digital signatures, distributed systems, law

11 Visually sealed and digitally signed documents

Vicky Liu, William Caelli, Ernest Foo, Selwyn Russell

January 2004 **Proceedings of the 27th conference on Australasian computer science - Volume 26 CRPIT '04**

Publisher: Australian Computer Society, Inc.

Full text available: pdf(665.30 KB) Additional Information: full citation, abstract, references

One of the primary flaws with current digital signature technology is that a digital signature does not "feel" or resemble a traditional seal or personal signature to the human observer; lacking a sense of visualisation and changing each time it is applied. This paper reviews the historical value of seals in Eastern and Western cultures to provide a basis to enhance global acceptability of existing digital signatures. The functionality of traditional seals is investigated in broad terms, encompa ...

Keywords: digital signatures, e-commerce, seal certificate, seals, security, verification, visualisation

12 Some cryptographic principles of authentication in electronic funds transfer systems

C. H. Meyer, S. M. Matyas

October 1981 **ACM SIGCOMM Computer Communication Review , Proceedings of the seventh symposium on Data communications SIGCOMM '81**, Volume 11 Issue 4

Publisher: ACM Press

Full text available: pdf(1.22 MB) Additional Information: full citation, abstract, references, citings, index terms

One essential requirement of an Electronic Funds Transfer (EFT) system is that institutions must be able to join together in a common EFT network such that a member of one institution can initiate transactions at entry points in the domain of another institution. The use of such a network is defined as interchange. Cryptographic implementations are developed for such a network in such a way as to keep personal verification and message authentication processes at diffe ...

13 Verifiable encryption of digital signatures and applications

Giuseppe Ateniese

February 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 1

Publisher: ACM Press

Full text available: pdf(258.12 KB) Additional Information: full citation, abstract, references, index terms

This paper presents a new simple schemes for verifiable encryption of digital signatures. We make use of a trusted third party (TTP) but in an *optimistic* sense, that is, the TTP takes part in the protocol only if one user cheats or simply crashes. Our schemes can be used as primitives to build efficient fair exchange and certified e-mail protocols.

Keywords: Certified e-mail, contract signing, digital signatures, fair exchange, proof of knowledge, public-key cryptography

14 Trust, recommendations, evidence, and other collaboration know-how (TRECK): How to incorporate revocation status information into the trust metrics for public-key

certification
Kemal Bicakci, Bruno Crispo, Andrew S. Tanenbaum
March 2005 **Proceedings of the 2005 ACM symposium on Applied computing**
Publisher: ACM Press
Full text available: pdf(124.41 KB) Additional Information: full citation, abstract, references, index terms

In a traditional PKI, the trust associated with a public key is expressed in binary either by 0 or 1. Alternatively, several authors have proposed trust metrics to evaluate the confidence afforded by a public key. However their work has a static point of view and does not take into account the issue of public key revocation. In this paper, we make the first attempt to incorporate the revocation status information into the trust metrics for public key certification. To achieve our goal, we use a ...

Keywords: PKI, public key certificates, revocation, trust metrics

15 Is hierarchical public-key certification the next target for hackers?
Mike Burmester, Yvo G. Desmedt
August 2004 **Communications of the ACM**, Volume 47 Issue 8
Publisher: ACM Press
Full text available: pdf(173.38 KB) html(27.53 KB) Additional Information: full citation, abstract, references, index terms

Considering alternatives to hierarchical authentication structures that are not sufficiently secure for communication on open networks such as the Internet.

16 Emerging applications: Defending against redirect attacks in mobile IP
Robert H. Deng, Jianying Zhou, Feng Bao
November 2002 **Proceedings of the 9th ACM conference on Computer and communications security**
Publisher: ACM Press
Full text available: pdf(266.04 KB) Additional Information: full citation, abstract, references, index terms

The route optimization operation in Mobile IP Version 6 (MIPv6) allows direct routing from any correspondent node to any mobile node and thus eliminates the problem of "triangle routing" present in the base Mobile IP Version 4 (MIPv4) protocol. Route optimization, however, requires that a mobile node constantly inform its correspondent nodes about its new care-of addresses by sending them binding update messages. Unauthenticated or malicious binding updates open the door for intruders to perform ...

Keywords: authenticated key-exchange, mobile IP, mobile IP security, redirect attack, secure binding update

17 Business: The 8th layer: Will the digital signature transform e-commerce?
Kate Gerwig
September 2000 **netWorker**, Volume 4 Issue 3
Publisher: ACM Press
Full text available: pdf(502.72 KB) html(13.80 KB) Additional Information: full citation, index terms

18 On the efficient implementation of fair non-repudiation
Cheng-Hwee You, Jianying Zhou, Kwok-Yan Lam
October 1998 **ACM SIGCOMM Computer Communication Review**, Volume 28 Issue 5

Publisher: ACM Press
Full text available: pdf(689.48 KB) Additional Information: full citation, abstract, citings, index terms

Due to the explosive growth of electronic businesses carried on the Internet, non-repudiation services turn out to be increasingly important. Non-repudiation services protect the transacting parties against any false denial that a particular event or action has taken place, in which evidence will be generated, collected and maintained to enable the settlement of disputes. Several fair non-repudiation protocols have been proposed, which support non-repudiation of origin and non-repudiation of rec ...

Keywords: dispute resolution, evidence chaining, fair non-repudiation, validity of evidence

19 SPV: secure path vector routing for securing BGP
Yih-Chun Hu, Adrian Perrig, Marvin Sirbu
August 2004 **ACM SIGCOMM Computer Communication Review , Proceedings of the 2004 conference on Applications, technologies, architectures, and protocols for computer communications SIGCOMM '04**, Volume 34 Issue 4
Publisher: ACM Press
Full text available: pdf(236.82 KB) Additional Information: full citation, abstract, references, index terms

As our economy and critical infrastructure increasingly relies on the Internet, the insecurity of the underlying border gateway routing protocol (BGP) stands out as the Achilles heel. Recent misconfigurations and attacks have demonstrated the brittleness of BGP. Securing BGP has become a priority.In this paper, we focus on a viable deployment path to secure BGP. We analyze security requirements, and consider tradeoffs of mechanisms that achieve the requirements. In particular, we study how to se ...

Keywords: BGP, Border Gateway Protocol, interdomain routing, routing, security

20 Legal, ethical, and societal issues in e-commerce: Driving off a tiger, but leading a wolf: a review of the Chinese contract law art.11
Yongjun Jin
August 2005 **Proceedings of the 7th international conference on Electronic commerce ICEC '05**
Publisher: ACM Press
Full text available: pdf(315.33 KB) Additional Information: full citation, abstract

With the purpose to get rid of the writing form barriers to E-Commerce, the Chinese Contract Law art.11 specified: "'Writing form' means a form, such as a contract instrument, letter, data message (including a telegram, telex, facsimile, electronic data interchange and electronic mail), that records the contract contents contained therein and is capable of being reproduced in tangible form."... Where the reduction to a tangible form is concerned, data message is not equal to contract instrument ...

Keywords: data message, electronic signatures, signatures, writing form

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2006 ACM, Inc.
Terms of Usage Privacy Policy Code of Ethics Contact Us

Useful downloads: Adobe Acrobat QuickTime Windows Media Player Real Player